City of Charlotte: 700 MHz Public Safety Wireless Broadband Network Interoperability Showing – FCC PS Docket 06-229

January 27, 2012 Version 2.1

REDACTED VERSION

Table of Contents

INTRODUCTION & BACKGROUND

This Interoperability Showing (IOS) Technical and Operational Response is intended to demonstrate the technical and operational proficiency of the City of Charlotte (the "City") necessary to achieve operability and interoperability of a public safety broadband network in accordance with Federal Communications Commission ("FCC" or the "Commission")May 12, 2010 (FCC 10-79) and December 10, 2010 (DA 10-2342) Orders, and its January 25, 2011Third Report and Order and Fourth Further Notice of Proposed Rule Making (FCC 11-6).

The City of Charlotte applied for and was awarded a grant to deploy a middle mile wireless broadband infrastructure for Public Safety and government use. The project will provide broadband access to Public Safety entities throughout the City as well as Mecklenburg County, North Carolina of which the City of Charlotte is a part. The City anticipates its network providing gateway services beyond its licensed geography becoming a cost-effective regional communications resource and an integral component of the nationwide public safety broadband network.

The project is being executed in cooperation with Alcatel-Lucent (ALU), who will deploy LTE technology, provide system operation, maintenance support, provisioning, billing, and customer support. In addition, the project will incorporate the sharing of networks, nationwide roaming, Public Safety priority of service, and provide a low cost tier of wireless data services as required by the Commission.

An objective of this system is to provide Public Safety agencies and other government users in the Charlotte/Mecklenburg area an interoperable broadband network to support a coordinated emergency response to any emergency. The system will provide government officials and first responders with many enhanced capabilities including, but not limited to, live streaming video capabilities, computer aided dispatch and automatic vehicle location, geo-location and situational awareness applications for tactical response, field-based reporting and image transfer, and real-time criminal database access.

The City of Charlotte's CharMeck Connect project proposes to deploy an interoperable 700 MHz Public Safety wireless broadband network for the city as well as the greater Mecklenburg County area. The system is designed to deliver 3 Mbps and 6 Mbps aggregate sector throughput for uplink and downlink connections respectively. These values are equivalent to the expected bandwidth, or capacity, available to all users within a single sector using the current 10 MHz spectrum allocation. At a minimum, CharMeck Connect will provide outdoor coverage at minimum data rates of 256 Kbps uplink (UL) and 768 Kbps downlink (DL), for a single user at the cell edge. The system will be capable of supporting the interoperability needs of emergency responders in the region as well as government services. The project plans to construct the network using both new and existing wireless towers and roof-tops and to bring thousands of Public Safety users onto the system.

The 3GPP standards-based LTE solution will support the set of applications defined by the National Public Safety Telecommunications Council (NPSTC) Broadband Task Force, and will also support a full spectrum of multimedia applications. The solution is being designed and is being implemented to interoperate with other 700 MHz Public Safety waiver recipients and also to become integrated as part of the National Public Safety Broadband Network.

The City of Charlotte asserts, at the conclusion of this InterOperability Showing (IOS), that its CharMeck Connect 700 MHz Public Safety Wireless Broadband Network is designed and is being implemented to meet or exceed the interoperability and other requirements of applicable FCC Report & Orders. CharMeck Connect will support Public Safety Sub-Network Mobility (formerly known as intra-system roaming) as of its Service Availability date on June 30, 2012.

The City of Charlotte has revised this IOS on January 27, 2012 to address: a) The FCC Order of January 9, 2012 (DA 12-25), and b) Answers to FCC questions from a call on January 19, 2012 (refer to City of Charlotte ex parte of same date). The City of Charlotte plans to revise or amend this IOS in mid-February 2012 to reflect evolving information from the PSST-OAC LTE Infrastructure Internetworking Group (IIG) and other interworking, administration and numbering coordination activities.

It is critical that the Commission work with CHARMECK in the completion of this InterOperability Showing (IOS) expeditiously as the City will host the National Democratic Convention in the summer of 2012. Since the President of the United States and other key dignitaries will be in attendance, the 700 MHz Public Safety Wireless Broadband Network is anticipated to be used by thousands of federal agents, state and local first responders to ensure the security of thousands of participants to this worldwide event.

SYSTEM OVERVIEW

High-Level Design

The City of Charlotte and Mecklenburg County are in progress of deploying a 700 MHz LTE network for their Public Safety personnel. This deployment results from a competitively procured contract with Alcatel-Lucent to provide LTE Core services via a Hosted model. The high-level design is shown in Figure 1 below, where the architecture is made up of three main components: the eUTRAN (evolved UMTS Terrestrial Radio Access Network), the microwave backhaul network, and the Evolved Packet Core (EPC or ePC).

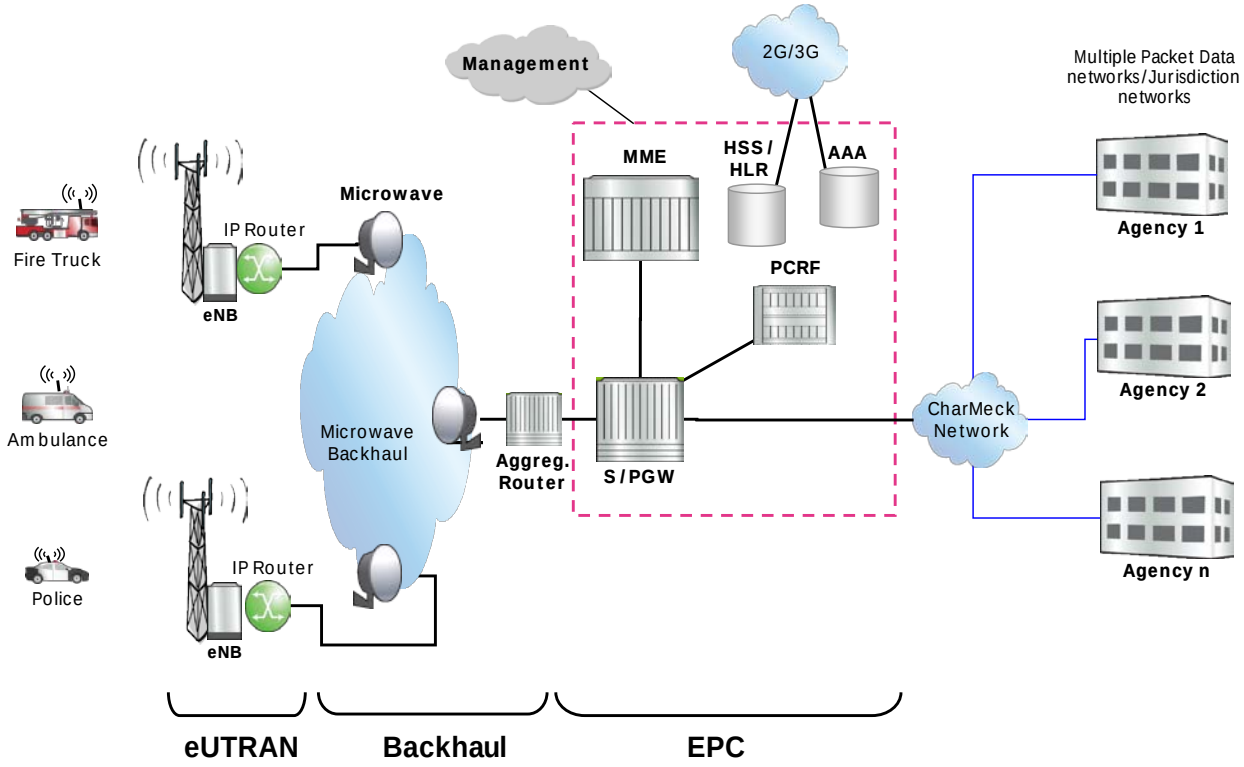


Figure 1 – High-Level Design Diagram

The eUTRAN component consists of the radio base stations (eNodeB or eNBs) which provide over-the-air connectivity to mobile terminals. The backhaul network consists of routers and microwave equipment. The ePC consists of the Mobility Management Entity (MME), a Serving Gateway, a Packet (data network) Gateway (S/PGW), the Home Subscriber Server (HSS), and the Policy & Charging Rules Function (PCRF). The ePC supports mobility functions (e.g., paging, authentication, location management, etc.) and connectivity to Public Safety networks to support the desired applications.

System Architecture

The City has chosen to implement a split hosted core model, where Alcatel-Lucent will host the majority of the ePC in a remote hardened facility, and will provide highly reliable service to the City via a negotiated service-level agreement. The City will purchase and own the eUTRAN component of the network, which consists of 39 eNodeB sites, as well as the microwave backhaul network which connects each of the sites together and to the City of Charlotte data network. In this split core hosted model, the S/P GateWays are owned by the City of Charlotte and are located at its central data center. The specific architecture and layout of the hosted solution is shown in Figures 2a and 2b.

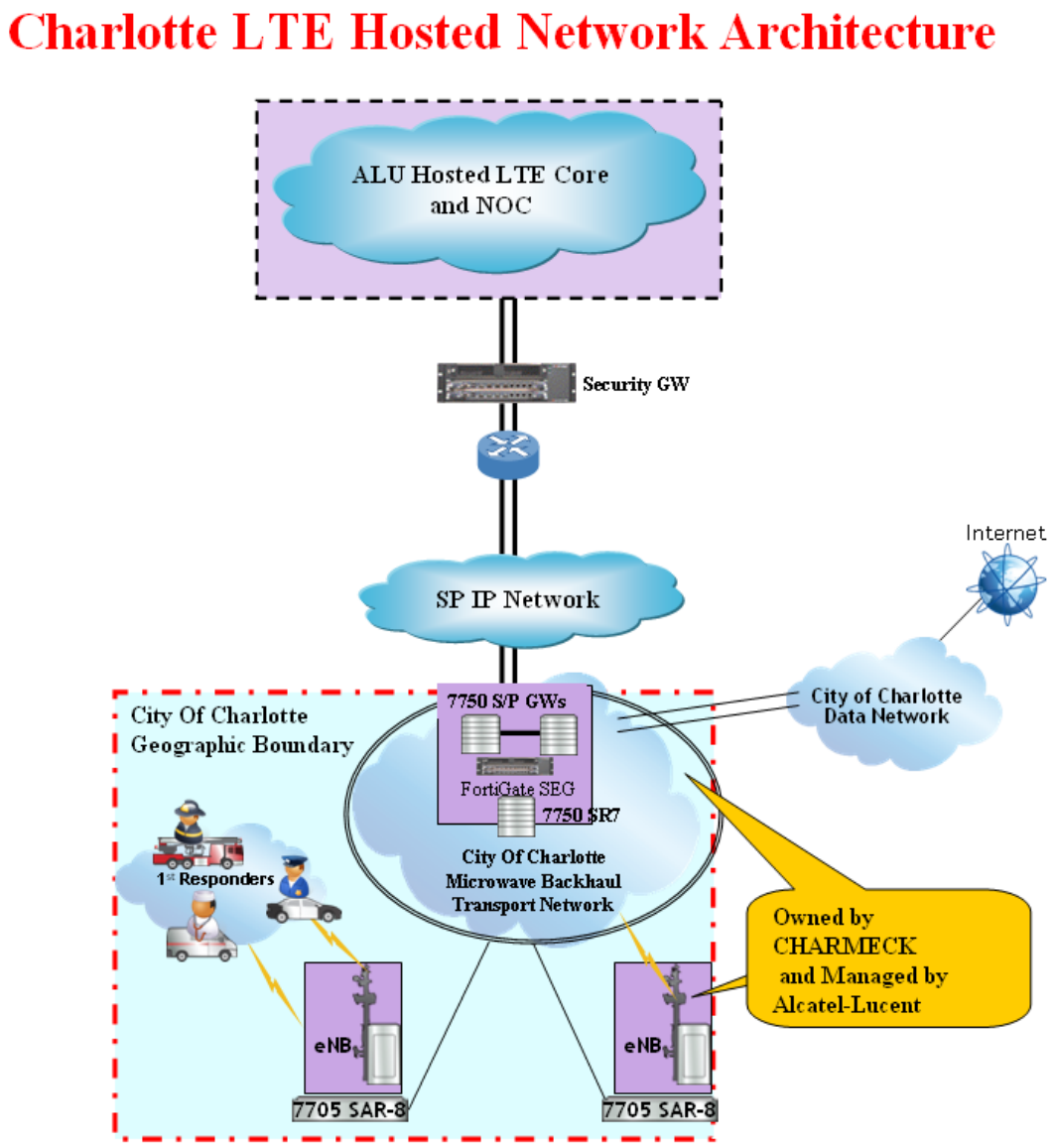


Figure 2a - Hosted LTE Architecture

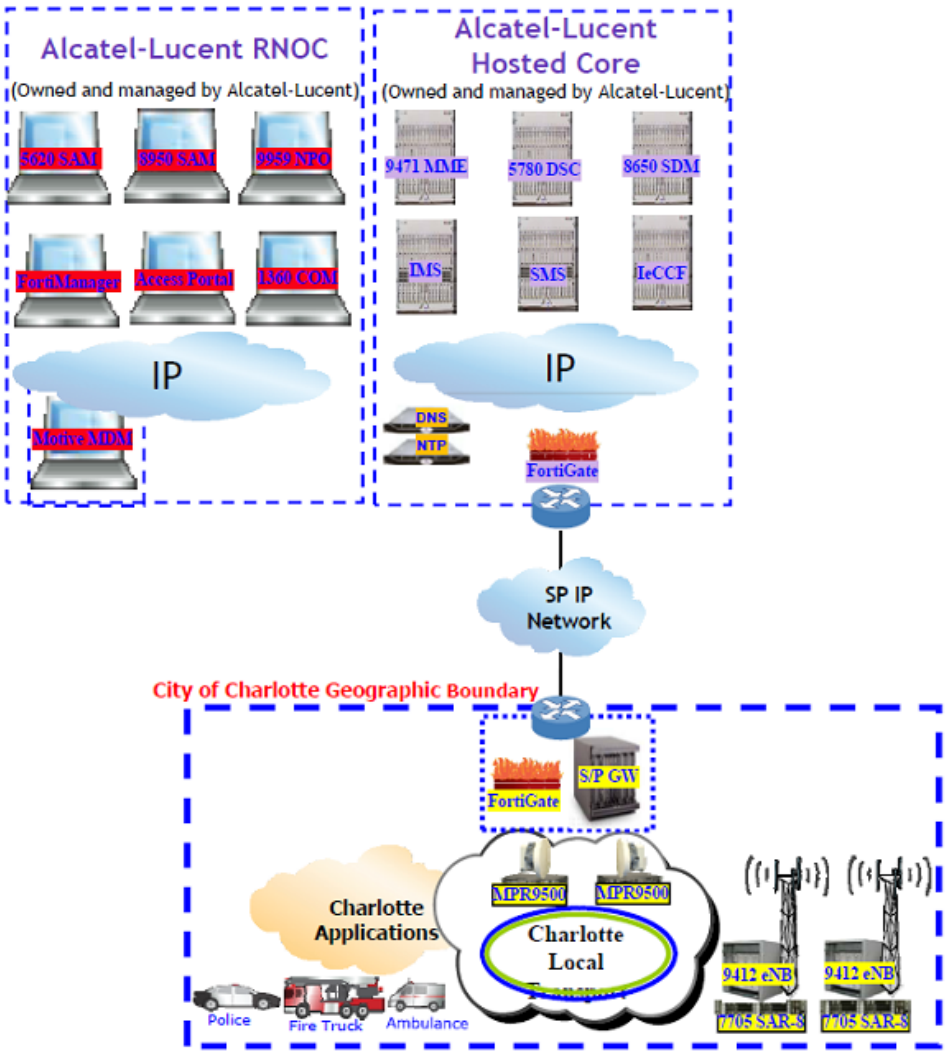


Figure 2b - Hosted LTE Architecture, Additional View

An important aspect of this architecture is that the City will purchase and own the Serving and Packet Gateways (S/P GWs) to maximize efficiency of the network and to maintain local routing and transport of user traffic. All (control and signaling) traffic transport towards the hosting facility is accomplished through the provision of two (2) physically diverse secure links from AT&T and Century-Link. Application network tie-in is indicated above in Figure 2b. Specific features and functionality of the Serving and Packet Gateways are described below.

SGW Functionality

The SGW (Serving Gateway) serves as the local mobility anchor for the User Equipment (UE) and terminates the packet data network interface towards the eUTRAN. The SGW is a data plane element whose primary function is to manage user-plane mobility. This means that packets are routed through the SGW for intra eUTRAN mobility and mobility with other 3GPP technologies, such as 2G/GSM and 3G/UMTS. All EPS bearers associated with an UE are established on the same SGW. SGW functionalities include:

- SGW Serves as the local mobility anchor for UE - terminates the packet data network interface towards the eUTRAN (UE).
- It manages user-plane mobility - performs IP routing and forwarding
- Local mobility anchor point for inter-eNodeB and inter-3GPP handovers
- Session supervision of the availability of the eNodeB
- Mobility anchoring for inter-3GPP mobility
- IDLE mode downlink packet buffering and initiation of network triggered service request procedure
- Packet routing and forwarding
- Accounting on user and Quality of Service (QoS) Class Identifier (QCI) granularity for inter-operator charging
- Uplink and Downlink charging per UE and per PGW

PGW Functionality

As an IP access gateway, the PGW terminates the SGi interface towards the PDN (packet data network), or IP network. It basically provides the user with a point of presence to the PDN or Internet. Other functionalities of the PGW:

- Provides the UE with an IP address
- Provides flow base charging under control of the PCRF
    - UL & DL service level charging (e.g. based on SDFs defined by the PCRF, or based on Deep Packet Inspection defined by local policy)
    - Serves as enforcement point for policy decisions coming from the PCRF
- Connects UE to PDN
- Serves as the cross technology mobility anchor
- Per user base packet filtering

Both gateways will be implemented with resilient routing hardware that provides for a full set of IPv4/IPv6 routing capabilities.

Partitioning, Security and Management for the Hosted ePC Core Tenants

The City of Charlotte understands that potential overcapacity and proliferation of ePC cores is being considered or pursued by some Waiver Recipients as well as others participating in these projects. The City believes this potential situation is not wise stewardships of the public's funds. As an economic alternative, the City is deploying a 700 MHz LTE network for their Public Safety personnel using a split hosted ePC core, as described above. In the planning and design phases of the LTE program, several security and partitioning aspects were addressed. These aspects are detailed here.

The City of Charlotte along with its primary vendor Alcatel-Lucent have designed and are implementing a split hosted ePC core for the 700 MHz Public Safety Wireless Broadband Network. This core is designed and is being implemented to meet or exceed the interoperability and other requirements of applicable FCC Report & Orders. The hosted core aspects of sharing and operation includes the following:

- The planned hosted core is dedicated to Public Safety only and not shared with commercial networks.
- There are no commercial carrier users. Commercial carrier signaling and traffic are not intermixed with Public Safety.
- Clear, definitive and secure partitions for tenants/jurisdictions are implemented.
- Capability for management and monitoring of multiple, concurrent instances (hosted ePC tenants) is afforded in a hierarchical manner with smaller divisions of domain as the levels go lower.
- Commonly accepted security and best practices are utilized, including tightly controlled authentication and access to management and other functions.
- Robust system redundancy is implemented throughout.
- Multiple levels of administration are allowed, including the ability to subdivide the domains of managed users within a jurisdiction. These administration capabilities yield tightly controlled visibility and access to subscriber data, allowing jurisdictions to manage their own subscribers (i.e., perform subscriber adds, changes, deletes, manage their priorities, and similar aspects).
- City of Charlotte will have 24x7x365 visibility and management capability in concert with Alcatel-Lucent.
- Clear separation between different ePC tenants or jurisdictions. The separations restrict hosted ePC tenants to visibility and management of only their own elements, objects and users.
- Operation and availability of the hosted core is defined by a service level agreement for each partitioned jurisdiction.
- Tenants (jurisdictions) are given the possibility to customize feature offerings for their subscribers.
- Logs of administrator actions are made available for auditing and to provide traceability for changes.
- Access Point Names (APNs) can be defined for each jurisdiction, providing members of a jurisdiction secure, walled access to their applications without other jurisdictions being able to access them.
- The ePC hosted core capabilities provide each jurisdiction with a view of the performance/occupancy of their set of eNodeBs.

Near-real-time call tracing capability to help monitor the performance of the system on a per-user and per-session basis through related metrics such as Radio resource Control (RRC) connections setup, service attach, service request, handovers, dropped packets, etc.

The hosted model allows the Network Operations Center (NOC) system administrator to define virtual network operators and authorized users in the hosted Element Management Systems (EMS) through a unique ID assignment. The Public Safety tenant's ePC hosted core requirements are defined and permissions granted in the hosted EMS prior to service activation. The hosted model provides secure access to workflows, work items, and user data through association with a service activator id. The service activator id represents an entity whose data is kept private from other users of the hosted platform. The service activator associated with the user id will control what workflows the user has access to on the EMS Graphical User Interface (GUI). This will include workflow creation and work item selection (search and view) via the

work item screen or the work list. The service group value will also determine what entries a user may view or update in any of the managed area.

The network is managed 24x7x365. Through a web portal, the City of Charlotte has access to dashboards which provide consolidated data views from various sources including fault, performance, trouble, provisioning, and billing tools. Key performance indicators, audit and access reports are also available.

Reliability, Resiliency and Survivability

The City of Charlotte hosted core LTE solution achieves high reliability through implementing a high degree of redundancy and resiliency at the network element level. The hosted core architecture allows for architecting a solution with no single point of failure. The principle in designing the redundancy architecture for the hosted solution is by provisioning enough network elements to meet the designed capacity of the hosted solution and additional redundant network elements for the desired level of reliability. Generally, all network elements with higher service impact in case of failure events will include more redundancy – for example, the core network of IP routers or the MME have more redundancy than the radio system access points. All hosted core network elements are internally redundant with automatic failover capabilities.

The hosted core site is connected through physically diverse links to the Serving and Packet GWs located in the City of Charlotte's data center. The connectivity consists of redundant transport circuits (ATT & Century-Link) for securely-routed signaling and management traffic.

All proposed ePC network elements are redundant with automatic failover capabilities, with minimal or no loss of state information during failover. Illustrations of such include, but are not limited to:

- The MME is based on a high-availability Advanced Telecommunications Computing Architecture (ATCA) hardware platform. The MME components support 1+1 redundancy.
- The SGW and PGW are built on the 7750 service router platform which also supports 1+1 redundancy.
- The PCRF is hosted on a fully redundant server platform.
- Some components in the HSS are 1+1 redundant, while N+N redundancy is provided for other HSS components.

The following Table highlights the various interfaces and the level of redundancy or duplex configuration for the nodes:

3GPP Interfaces	Redundancy/Duplexing	End points
S6a – Visited MME to Home HSS;	n/a	ALU
S9 – Visited PCRF to Home PCRF for dynamic policy arbitration – note that with a single PLMN ID for all public safety networks this interface is not used to roam between public safety networks;	n/a	ALU
S10 – MME to MME support for Category 1 handover support;	n/a	ALU
S1-u – between eNodeB and SGW;	Redundant transport	Charlotte
S1-MME – between eNodeB and MME;	Geo-diverse connection(1)	Charlotte/ALU
S5 – between SGW and PGW;	Duplex configuration	Charlotte
S6a – between MME and HSS;	Duplex configuration	ALU
S11 – between MME and SGW;	Geo-diverse connection(1)	Charlotte/ALU
SGi – between PGW and external PDN;	LAG connection	Charlotte
Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules);	Geo-diverse connection(1)	ALU
Rx – between PCRF and AF located in a PDN;	Geo-diverse connection(1)	Charlotte/ALU
Gy/Gz – offline/online charging interfaces.	Duplex Configuration	ALU
Uu- LTE air interface;	contingent on cell overlap	Charlotte
X2 – eNodeB to eNodeB;	transport is redundant	Charlotte
S8 – Visited SGW to Home PGW – note that with a single PLMN ID for all public safety networks this interface is not used to roam between public safety networks;	n/a	n/a

(1) The geo-diverse connectivity will be achieved through secured leased links from AT&T and Century-Link providers

Coexistence of the Hosted ePC Core Model With Other Models

The City of Charlotte along with its primary vendor Alcatel-Lucent are implementing the split ePC hosted core not only to meet or exceed FCC interoperability and public safety requirements, but also to coexist with other models as these other models are being implemented by other Waiver Recipients. Furthermore, the architecture and design work are being executed in a manner which embraces future migration into the anticipated, larger National Public Safety Broadband Network.

The system, as designed and implemented, is based on 3G Partnership Project (3GPP) standards. As such, it is designed to interoperate and coexist with other models. Under the planned hosted core model, as reflected in this document, 3GPP standard interfaces are implemented to ensure interoperability with other types of network deployments, regardless of whether they are based on a hosted service or not. The systems are Internet Protocol versions 4 and 6 compliant. Industry standard protocols, interworking and best practices are used throughout.

The City of Charlotte along with its primary vendor Alcatel-Lucent are collaborating extensively with other jurisdictions, early implementers and other vendors to meet the above objectives for coexistence and interoperability. Coexistence and interoperability are further extended by incorporation of Internet Packet Exchange (IPX) services providers, such as those used and

proven out by commercial carriers. Furthermore, to the extent that Public Safety Communications Research (PSCR) recommendations and guidance are available, the City and ALU have incorporated such findings into the CharMeck Connect designs. Examples of coexistence and interoperability collaboration include, but are not limited to:

- Frequent (weekly) participation in Public Safety Spectrum Trust Operator Advisory Committee (PSST-OAC) activities;
- Leadership and weekly participation in the PSST-OAC LTE Infrastructure Internetworking Group (IIG);
- Designs incorporate or factor in National Public Safety Telecommunications Council (NPSTC) Broadband Task Force initiatives;
- Incorporation of PSCR findings and guidance;
- The City of Charlotte is actively working on a weekly basis with Harris County Texas on early interworking and interconnection efforts.

CITY OF CHARLOTTE'S RESPONSE TO SPECIFIC TECHNICAL INTEROPERABILITY REQUIREMENTS

Each of the sections below outline the specific technical interoperability requirements recommended by the Commission's Emergency Response Interoperability Center (ERIC) and Ordered by the Public Safety and Homeland Security Bureau in the Waiver Order FCC 10-79 (May 12, 2010), Third Report and Order and Fourth Further Notice of Proposed Rulemaking, FCC 11-6 (January 26, 2010) , Order DA 10-2342 (December 10, 2010) and the Order DA 12-25 January 9, 2012, followed by the City's response.

Public Safety Roaming on Petitioners' Networks

Requirements

The FCC requires that technical roaming capability, for both home-routed traffic and local breakout traffic, must be available on the date that a Petitioner's network achieves service availability. A Petitioner who achieves service availability should be required to certify its compliance with this condition in the following quarterly report.

The FCC also requires that all Petitioners honor each others' written requests to support roaming. If parties are unable to reach a roaming agreement within ninety days of the date a request is made, either party should have the option of referring the matter for Commission review and action.

City of Charlotte Response

The City of Charlotte will support Public Safety Sub-Network Mobility (previously referred to as roaming) of visiting Public Safety users with appropriate 3GPP compatible user equipment onto CharMeck Connect 700 MHz Public Safety Network on or after its Service Availabilty Date on June 30, 2012. The City will enter into reciprocal roaming agreements with other waiver recipients, as well as agreements with State, Local and Federal law enforcement and emergency responder agencies that request inter-operational (roaming) access.

Intra-State Coordination

The CharMeck Connect 700 MHz system being implemented by the City of Charlotte and Mecklenburg County is the only known 700 MHz system to be implemented in North Carolina through 2014. The City of Charlotte is committed to working closely with the State of North Carolina to develop a process to coordinate with and support interoperability with Public Safety users and other waiver recipients within the State of North Carolina. Currently, the City of Charlotte has a lead role and coordination discussions are in process with the StateWide Interoperability Coordinator (SWIC) and the State of NC Chief Information Officer's (CIO) office. City of Charlotte is in possession of a letter from State of NC CIO documenting existence of coordination.

Inter-State Coordination

The City of Charlotte is committed to working closely with the State of North Carolina to develop a process to coordinate with and support interoperability with Public Safety users and other waiver recipients from outside the State of North Carolina.

In order to stay consistent with other interoperating entities, the City expects to develop a process similar to that outlined by the State of Texas in their interoperability showing (November 4, 2011 v8.0 Section B.3 'Inter-State Processes) for coordinating with out-of-state interoperability partners. Partial excerpt follows.

Out-of-state FCC 700 MHz Public Safety broadband waiver recipients wishing to connect to CharMeck Connect shall make a request to the City, in which the requester shall include, at a minimum, documentation proving that requester: 1) Has been granted an FCC 700 MHz Public Safety broadband waiver for a specific geographic area; 2) Has a valid spectrum lease with the PSST, which has been approved by the FCC; 3) Provides technical information necessary to support Home Packet GateWay Access (HPA) [accessing Home APNs from visited sub-network] and Local Packet GateWay Access (LPA) [accessing common APNs via local PGWs in a visited sub-network]. {{These were formerly known as Home Routing (routing to PGW in Charlotte jurisdiction) and Local Breakout access (routing to PGW in visiting network)}} and; 4) Agrees to conform with all current and future FCC Orders pertaining to 700 MHz Public Safety broadband interoperability. The City will directly inform current and future FCC Waiver Recipients on how to make a request, and provide regular feedback as to the status and progress of their request.

Public Safety Spectrum Trust Operating Advisory Committee LTE Infrastructure Internetworking Group (IIG)

The City of Charlotte is a leading participant in the LTE IIG. The LTE Infrastructure Internetworking Group (IIG) is a team of industry consultants, LTE infrastructure providers and network operators selected by the Public Safety Spectrum Trust Operator Advisory Committee (PSST-OAC) to develop recommendations, guidelines and reference architectures for internetworking and a plan by which the PSST-OAC jurisdictions can establish internetworking. The City of Charlotte plans to adhere to these recommendations and reference designs. As such, much of the interworking related information in this Interoperability Showing is based upon the determinations of the LTE IIG.

The LTE Infrastructure Internetworking Group (IIG) has refined and evolved some of the terminology surrounding the architecture of the Public Safety Broadband Network. The evolution of the terminology stems from and is based on the Common PLMN ID approach as required by the Commission. This terminology refinement is further explained in Appendix B.

The IIG will deliver to the PSST-OAC recommendations on:

- A scalable network architecture for internetworking of LTE infrastructures provided by different manufacturers (e.g. S&P Gateways, MMEs, HSS, etc), assuming a single PLMN identification number will be used for the initial public safety deployments;
- Guidelines for employing 3GPP standards and interfaces (e.g. S6a, S5, etc.) needed to support the design and feature functionality to ensure internetworking between diverse

LTE infrastructures; and

- Interconnectivity options and intra-system roaming capabilities between public safety LTE EPCs.

Recommendations are vendor agnostic and rely on standards that are achievable by IPX, infrastructure and integral service providers. The IIG will present its recommendations to the PSST-OAC on or before February 2, 2012. The City of Charlotte will amend this Interoperability Showing in early February to incorporate these recommendations as appropriate.

PLMN ID Assignment

The National Public Safety Telecommunications Council (NPSTC) Broadband Task Force has recommended that the number of Public Land Mobile Network IDentifiers (PLMN IDs) allocated for a nationwide Public Safety broadband network should be less than 100, and may be as few as one. The Public Safety Communications Research (PSCR) NIST organization has recommended a common (single) PLMN ID. The implementation of the CharMeck Connect 700 MHz system will support this Common PLMN ID recommendation. The City will follow and comply with January 9, 2012 FCC Order DA 12-25 that a Common PLMN ID be implemented for the nationwide Public Safety broadband network. The City believes that a Common PLMN ID will simplify Public Safety Sub-Network Mobility (previously referred to as roaming) of Public Safety users across a nationwide network, yet still allow for identification of regional networks through the partitioning of subscriber (MSIN) identification numbers.

The City of Charlotte will implement, prior to its date of service availability on 6/30/12 a common PLMN ID that the ATIS IMSI Oversight Council (ATIS IOC) designates for the 700 MHz public safety broadband network. The implementation of a Common PLMN ID was assumed previously as stated in this Interoperability Showing. Substantial high-level and low-level design work has been completed based upon this requirement.

IMSI Numbering Schema

During 2011, the State of Texas along with other Waiver Recipient stakeholders and the Public Safety Communications Research (PSCR) program have recommended PLMN and IMSI numbering schema within a common (single) PLMN ID. During November 2011 through January 2012, under purview of both PSST-OAC and PSCR, an attempt was made to homologate these into a final scheme. Nonetheless, FCC Order of January 9, 2012 DA 12-25 requires adoption of the PSCR schema but allows certain flexibilities. The implementation of the CharMeck Connect 700 MHz system will be based on these FCC requirements.

The Public Safety Spectrum Trust Operating Advisory Committee has chartered a Numeric Identifier working group. This working group will complete the development of the numbering schema by using the PSCR guidelines as the basis and then modify with certain flexibilities granted by the FCC. This working group also will, in the near future, design preliminary processes that could be used by the numbering administrator. The PSST-OAC, in concert with its Numeric Identifier working group, is actively pursuing an option to utilize and contract with a subcontractor to DHS-OEC for a numbering administrator. The PSST-OAC Numeric Identifier working group is devising a Statement Of Work to become part of the contract with the numbering administrator.

The City of Charlotte supports the above initiatives and will use the outcomes as a basis of system design and operation once acceptable or approved by the FCC. City of Charlotte has been and is currently a participant in the PSST-OAC Numeric Identifier working group for the implementation of the numbering schema. Charlotte, with this working group and with other Waiver Recipients, will collectively implement the schema for the assignment of IMSIs and other identification numbers necessary to support all of the Waiver Recipients' operations of LTE broadband deployments on an interoperable basis.

Multiple HSS

The City of Charlotte is deploying CharMeck Connect with a Home Subscriber Server (HSS) in an ePC core hosted by Alcatel-Lucent. Other early 700 MHz system deployments are similarly utilizing their own HSS and related systems. This approach works well from an interoperability perspective since DIAMETER protocols and routing integrate multiple HSS's. The City of Charlotte will have an HSS for its Public Safety Sub-Network known as CharMeck Connect. This sub-network is a subset of the Public Safety Broadband Network and is defined by an IMSI/MSIN range within the Common (single) PLMN-ID. A sub-network provides an HSS for its particular IMSI Range within the Common PLMN ID. The National Network is subdivided into Sub-Networks based on IMSI ranges within the Common (single) PLMN-ID. By definition, each Sub-Network is operated by a different Public Safety agency or agencies. DIAMETER protocols and routing (DRA) ensure that MME's and other infrastructure know the appropriate HSS to work with.

Public Safety Sub-Network Mobility

Public Safety Sub-Network Mobility (formerly known as Intra-system roaming) occurs when other Public Safety users obtain service from a visited regional portion of the nationwide network which is not part of their home region. CharMeck Connect will support Sub-Network Mobility or intra-system roaming as of its Service Availability date on June 30, 2012.

The City of Charlotte plans to adopt and implement recommendations of the Public Safety Spectrum Trust Operating Advisory Committee LTE Infrastructure Internetworking Group (IIG) with regard to Public Safety Sub-Network Mobility. The City of Charlotte will support both Home Packet Gateway Access (HPA) [accessing Home APNs from visited sub-network] and Local Packet Gateway Access (LPA) [accessing common APNs via local PGWs in a visited sub-network] as of its Service Availability date.

Specifically, Charlotte is planning to leverage an "Internetwork Packet Exchange" (IPX) to provide sub-network mobility in phase 1, as well as inter-system roaming in phase 2. Phase 1 and Phase 2 are clarified in Appendix C. This is the leading, endorsed recommendation from the PSST-OAC IIG. However, Charlotte is closely monitoring the IIG activity and will consider adopting other proposals coming out of that activity if different. The IPX functionality leveraged for intra-system roaming is as follows:

- "DIAMETER Edge Agent" (DEA) / "DIAMETER Routing Agent" (DRA) to handle the routing of S6a and S9 messages between the commercial network and the particular waiver recipient network
- Central "Domain Name Server" (DNS) to expose waiver recipient network DNS records

- Network edge router that supports "Border Gateway Protocol" (BGP) to advertise IP routes and forward traffic flows to the particular waiver recipient network

The technical solution is outlined in the Figure 3.

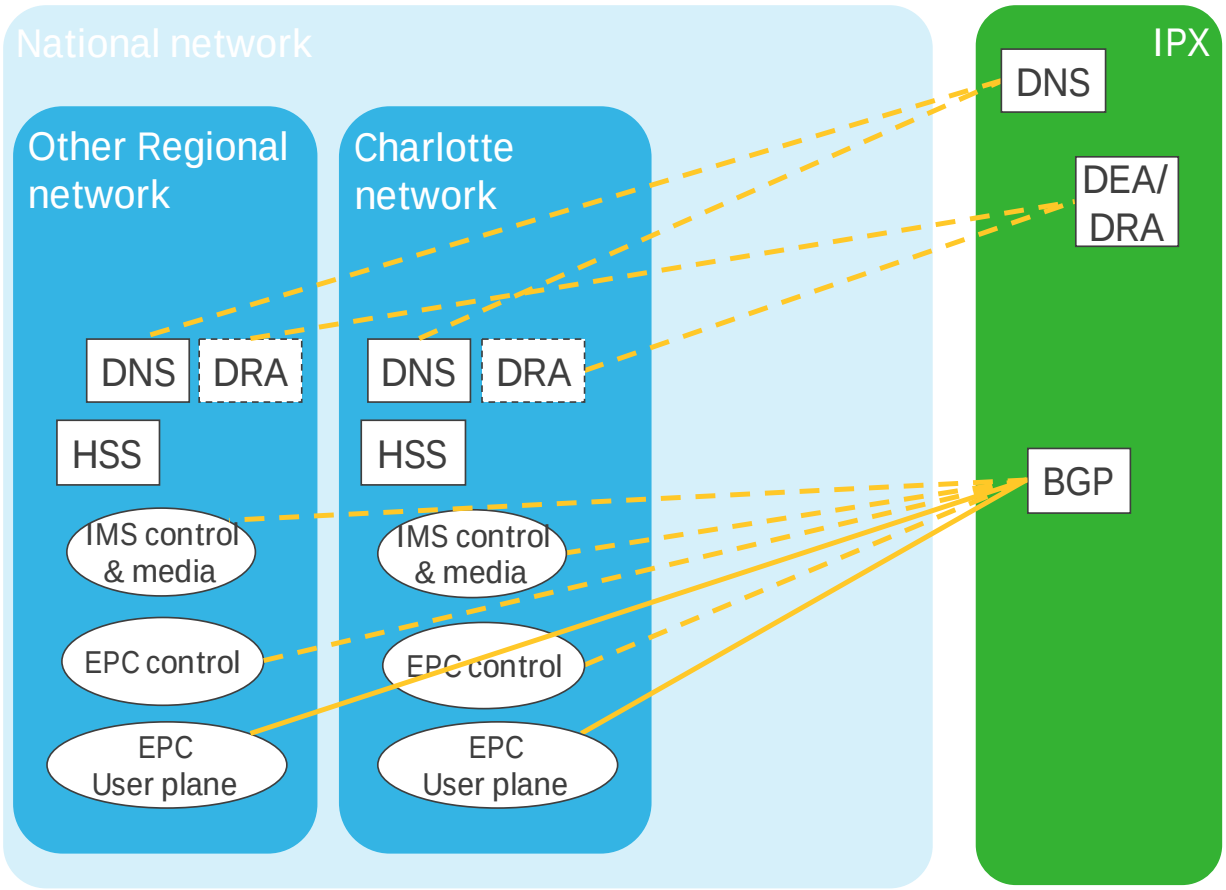


Figure 3 – Intra-System Roaming Interfaces

From an operational viewpoint the IPX "DEA/DRA" node will be configured to route incoming S6a messages to the correct waiver recipient network. This will be based on the International Mobile Subscriber Identity (IMSI) number. Therefore, an agreement is required between waiver recipients regarding the allocation of blocks of the Mobile Station Identification Number (MSIN) field to individual waiver networks. It is possible that this will be based on the top 3 digits of the MSIN, corresponding to the 7th, 8th and 9th digits of the IMSI, but this is not required. Discussions with the IPX providers indicate this is functionality they can provide. Also, the IPX BGP router function would require either manual or automatic establishment of IP routes to the individual waiver recipient networks.

The City of Charlotte and the PSST-OAC IIG are currently in detailed discussions with 3rd Party IPX Service Providers to establish the above functionality and recommends that the other Waiver Recipients share this facility. The PSST-OAC is actively considering this as an option. The City of Charlotte had previously, in December 2011 and in conjunction with the PSST-OAC IIG,

initiated a Request For Information (RFI) regarding IPX Interworking and Network Services.

Sub-Network Mobility Session Initiation

Public Safety roaming partners utilizing user equipment (UE) compliant with 3GPP R8 standards will be able to roam across regionally deployed public safety networks.

After authentication on a visited network, an IP address is assigned, and the intra-system roaming partner then has the ability to access IP services. If an HPA session is initiated, then the home network assigns an associated IP address to the UE. If an LPA local session is initiated, the visited network assigns an associated IP address to the UE.

Inter-System Roaming

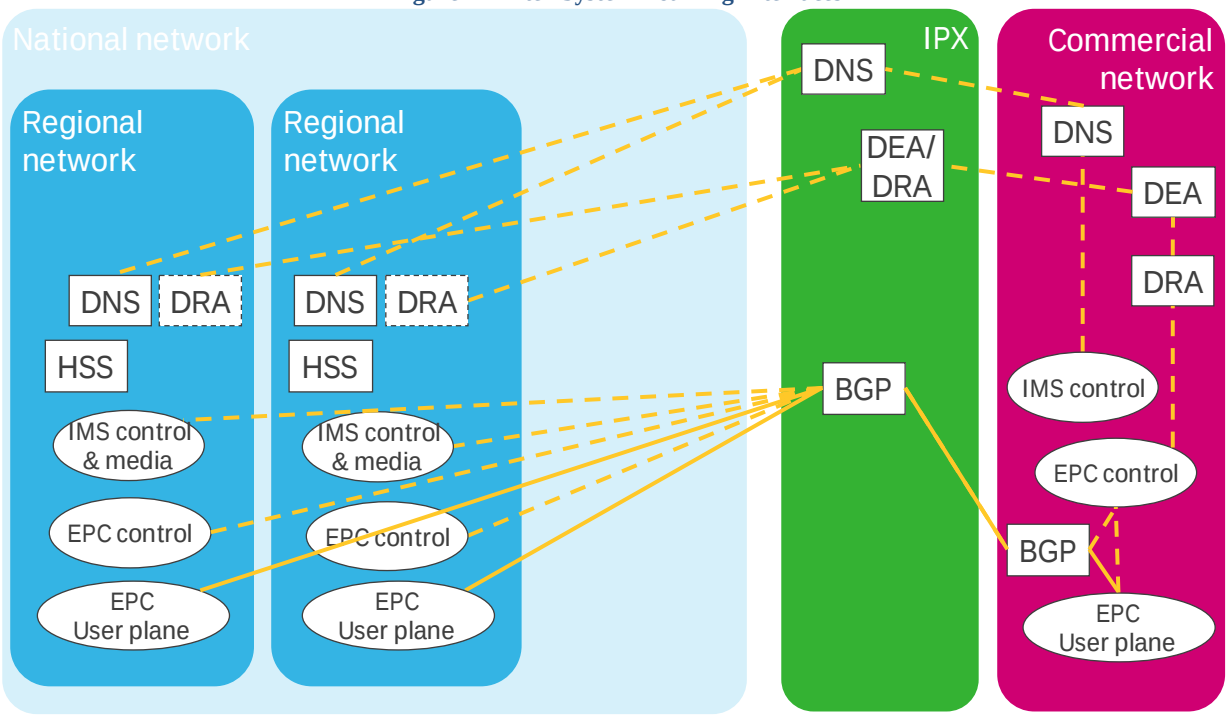
Inter-system roaming occurs when Public Safety users obtain service from a commercial carrier network, which is not part of the Public Safety nationwide network. The obvious implication is that this involves a different network PLMN ID. CharMeck Connect will support inter-system roaming in phase 2 of the deployment as enabled by roaming agreements with one or more commercial carriers. The City of Charlotte has initiated discussions with at least two large wireless carriers. The City of Charlotte plans to use the well known specifications and agreements from the GSM Association (GSMA) as the basis for inter-system roaming on to a commercial network. This solution will build on the initial IPX configuration above, adding requirements for the distribution of roaming charges and the handling of payment (ie 'Clearinghouse'; not shown in figure below).

Commercial Roaming (equivalent to Public Safety Inter-System Roaming) does not currently exist. Therefore, this City of Charlotte and IIG workscope is currently scheduled beyond February 2012. Furthermore, Public Safety Inter-System Roaming is highly dependent upon availability of devices which support the commercial band(s) and mode(s), such as HSPA,EV-DO, etc. At the time of this writing, these devices generally do not exist.

The Clearinghouse functionality (January 9, 2012 FCC Order DA 12-25) is built into this solution. The City of Charlotte had previously, in December 2011 and in conjunction with the PSST-OAC IIG, initiated a Request For Information (RFI) regarding IPX Interworking and Network Services. An RFI objective is to arrange for a common competent clearinghouse to support commercial roaming by all of the Petitioners. Inter-system commercial roaming has been anticipated and substantial high-level and low-level design work has been completed based upon these requirements. Support for such will be in Phase 2.

Figure 4 shows the planned commercial roaming architecture.

Figure 4 – Inter-System Roaming Interfaces



Applications

In accordance with the requirements of the waiver recipients, CharMeck Connect will support all system applications of the FCC 3rd Order, including the following applications for applicable users:

- Internet access
- VPN access to any authorized site and to home networks
- a status or information "homepage;"
- access for responders under the Incident Command System, and
- field-based server applications.

The City of Charlotte, in concert with the PSST-OAC LTE IIG design work group and Alcatel-Lucent hosted ePC core architects and engineers are currently in low level design of the network systems which will implement the above applications. Access Point Names (APNs) are defined as recommended or required. Secured, walled access to applications is provided using generally accepted information technology and networking protocols and technology. Security measures are further detailed below. The City of Charlotte will support applications as required by the applicable FCC Orders. The City of Charlotte will support both Home Packet Gateway Access (HPA) [accessing Home APNs from visited sub-network] and Local Packet Gateway Access (LPA) [accessing common APNs via local PGWs in a visited sub-network] as of its Service Availability date.

Technology Platform and System Interfaces

Requirements

In addition to the interfaces required in the *700 MHz Waiver Order*, Petitioners' systems should also be required to support a range of interfaces necessary to ensure the interoperability of equipment and devices manufactured by different vendors. Specifically, the FCC requires that Petitioners' systems support the following interfaces:

- S1-u – between eNodeB and SGW
- S1-MME – between eNodeB and MME
- S5 – between SGW and PGW
- S6a – between MME and HSS
- S11 – between MME and SGW
- SGi – between PGW and external PDN
- Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules)
- Rx – between PCRF and AF located in a PDN
- Gy/Gz – offline/online charging interfaces

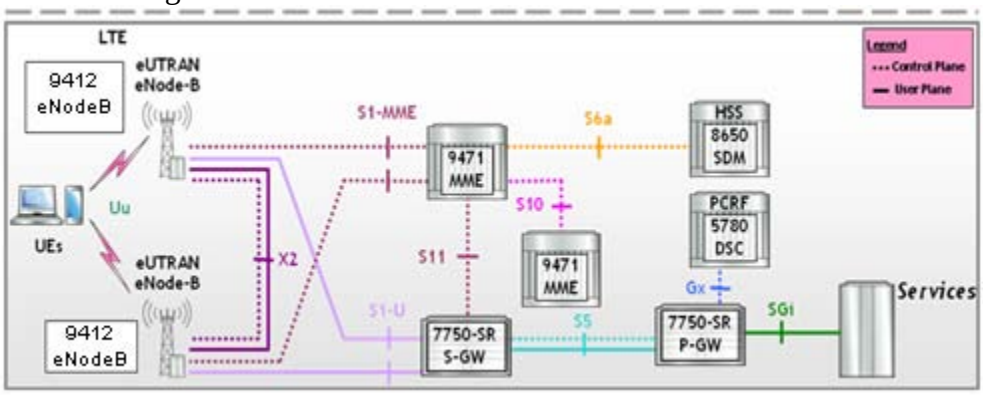
Additionally, Petitioners are allowed to utilize both IP version 4 (IPv4) and IP version 6 (IPv6) in their early-deployed networks.

City of Charlotte Response

CharMeck Connect will provide all interfaces necessary to ensure roaming and interoperability from other regional Public Safety broadband networks, specifically those interfaces required by the FCC 3rd Order. The system shall support the following Release 9 interfaces and will support future LTE releases as they become commercially available:

- Uu- LTE air interface;
- S6a – Visited MME to Home HSS;
- S8 – Visited SGW to Home PGW – note that with a single PLMN ID for all public safety networks this interface is not used to roam between public safety networks;
- S9 – Visited PCRF to Home PCRF for dynamic policy arbitration – note that with a single PLMN ID for all public safety networks this interface is not used to roam between public safety networks;
- S10 – MME to MME support for Category 1 handover support;
- X2 – eNodeB to eNodeB;
- S1-u – between eNodeB and SGW;
- S1-MME – between eNodeB and MME;
- S5 – between SGW and PGW;
- S6a – between MME and HSS;
- S11 – between MME and SGW;
- SGi – between PGW and external PDN;
- Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules);
- Rx – between PCRF and AF located in a PDN;
- Gy/Gz – offline/online charging interfaces.

In line with the 3GPP standard network architecture, and from a logical implementation, the key network elements supported by the system and the interface between these elements are shown in the figure below:



CharMeck Connect plans to initially deploy IPv4. However, the solution is fully capable of supporting IPv6 as well. Significant network partitions will utilize IPv6 as of Service Availabilty date. In addition, when other public safety users visit the CharMeck Connect network using an Access Point Name (APN) routing back to their home network they can use IPv6 addresses for that APN if desired. CharMeck Connect plans to evolve to IPv6 once its applications can be validated and adapted if necessary to function in an IPv6 environment.

System Identifiers

Requirements

Compliance with 3GPP standards requires that public safety broadband networks be assigned Public Land Mobile Network (PLMN) identification (ID) numbers. The FCC requires each Petitioner to submit notice to the Commission of its need for a PLMN ID. The FCC will then work with that Petitioner to determine an appropriate course for obtaining a PLMN ID.

City of Charlotte Response

The timeline for the implementation of CharMeck Connect is shown at high level in Appendix C. It can be seen that the key "go live" date for Phase I of CharMeck Connect is June 30th of 2012. This schedule is required in order to meet the need for the Democratic National Convention (DNC) in the summer of 2012. Therefore, the City requires a Public Land Mobile Network (PLMN) IDentification (ID) number (PLMN ID) in mid to late February 2012. CharMeck Connect will support FCC requirements for a Common PLMN ID.

Conformance Testing

Requirements

The FCC requires that conformance testing, a process generally planned and developed by industry organizations and conducted at certified laboratories, be implemented for Petitioners' early-deployed networks to ensure that devices and equipment deployed in the public safety broadband spectrum comply with Release 8 (LTE) and higher of 3GPP standards.

The FCC recognizes that a formal conformance testing process for LTE Band 14—which includes the public safety broadband spectrum—is not available. However, the FCC notes that the PCS-Type Certification Review Board is expected soon to complete development of such a process. The FCC requires that, within six months of either (1) the Commission or Commission's release of a public notice announcing the availability of the PTCRB testing process for Band 14, or (2) the Petitioner's date of service availability—whichever date is later—each Petitioner shall certify to the Commission that it has completed this process in consultation with a certified laboratory. In this certification, each network operator should also be required to commit to any future testing called for within the certification process.

City of Charlotte Response

The City of Charlotte LTE network will be 3GPP Release 9 upon Service Availability. Devices operating on the network will be Release 8 at a minimum. It is anticipated that a majority of devices will be in conformance with Release 9 specifications.

A comprehensive Acceptance Testing Procedure ("ATP") has been established for CharMeck Connect which will include a demonstration of coverage, capacity and all functionality from the Radio Access Network (RAN), through the aggregation network and the core. At a minimum, the following functional and operational tests will be performed prior to acceptance:

- System Functional Test,
- Subscriber Functional Test,
- Coverage Testing,
- System Baseline/Utilization (Throughput test),
- Security,
- Fault Management, and
- 30-Day Stability/Soak Test ("Burn-In") [Phase 2].

The ATP complies with the requirements and standards as published by the National Institute of Standards and Technology (NIST) Public Safety Communications Research (PSCR) laboratory and 3GPP. The City has also dictated the following requirements:

- The City requires that all broadband infrastructure components and all subscriber equipment shall have been subjected to testing as defined in the 3GPP standards:
- The City requires all standards compliance documentation to be provided prior to commencement of Factory Acceptance Testing,
- The City requires demonstration that all infrastructure and subscriber units are in full compliance with 3GPP and PSCR specifications. Standards conformance testing must

be based on 3GPP test suites that are developed by the PCS Type Certification Review Board ("PTCRB") or, if not yet available, on testing mutually agreed to be the City and the supplier. Testing shall include demonstrating multiple vendors' subscriber units operating on the infrastructure, subject to interoperability agreement with those vendors.

- The City requires that the ATP will include tests that demonstrate compliance with all system functional requirements via a selection of at least 50 test cases.
- A test of the capacity of the System shall be conducted. The system is designed to meet the required capacity. Note that, the system has also gone through extensive testing in the staging phases before deployment.

Interoperability Testing

Requirements

Interoperability testing (IOT) is an important mechanism for ensuring that public safety broadband networks are technically capable of supporting roaming, a central component of interoperability. The FCC requires Petitioners to perform IOT for the LTE interfaces necessary to support roaming. These include:

- U_u – LTE air interface
- S6a – Visited MME to Home HSS
- S8 – Visited SGW to Home PGW
- S9 – Visited PCRF to Home PCRF for dynamic policy arbitration

In the quarterly report following its date of service availability, each Petitioner is required to submit a plan for conducting IOT on the interfaces specified above for Commission approval. The scope of testing outlined in the plan should be sufficiently broad to address all of the capabilities and functions required by the *Waiver Order*. Additionally, the plan should commit to testing on a regular basis with other Petitioners' networks that have achieved service availability. The FCC requires that the Petitioners update the Commission on their progress with IOT in their quarterly reporting.

City of Charlotte Response

Infrastructure

The CharMeck Connect infrastructure equipment supplier, Alcatel-Lucent (ALU) has done extensive interoperability testing of its equipment in various commercial environments and test beds such as those coordinated by the Multi-Switch Forum (MSF). ALU has and continues to be a very active supporter of the NIST PSCR demonstration network. ALU was the first vendor operational in that network, and have passed all phases currently defined (1 and 2a).

ALU has tested the S6a interface with their own infrastructure, as well as other vendor's Home Subscriber Servers (HSS) and has deployments in operation today in commercial networks. ALU also has a device interoperability (IODT) lab which tests LTE devices for standards compliance and performance, and have validated the Uu interface with many devices to date, and are actively testing B14 devices. As mentioned above, the S8 and S9 interfaces will not likely apply to a public safety network that uses a Common PLMN ID. However, Alcatel-Lucent already has

done interoperability testing for S8 and is ready to do additional testing as required.

Devices

The City of Charlotte has issued a Request For Proposal (RFP) for LTE-compliant devices. The City is evaluating the responses and has selected multiple vendors to move forward. Once their devices are certified, the vendors will be eligible to supply devices for use on CharMeck Connect. To become certified, the City is requiring that all UE proposed for CharMeck Connect must be certified by Alcatel-Lucent InterOperability Device Testing (IODT) prior to procurement of such devices by the City.

The City of Charlotte has opened the procurement process and decision making to other jurisdictions as part of a cooperative purchasing mechanism. Currently, there are three other Waiver Recipients involved in this purchasing coop effort.

The PSCR envisions using the Multiservice Switching Forum (MSF) as a body to perform conformance testing on the key network interfaces required in the PSBN. Alcatel-Lucent has been fully engaged in the PSBN testing processes in the PSCR demo network. They are also a member of the MSF as well as the Network Vendors' Interoperability Testing Forum (NVIOT), and have participated in several LTE IOT events sponsored by those groups already.

Operation of Fixed Stations

Requirements

The 700 MHz public safety broadband spectrum has excellent propagation characteristics for mobile wireless broadband services. However, the wide-spread use of this spectrum for fixed operations could complicate the interference environment of an early-deployed network, and adversely impact its operability and interoperability, by potentially limiting network access for mobile users at crucial times or in emergency situations. The FCC recommends that operation of fixed stations in early-deployed networks be permitted only on a secondary, non-interference basis to mobile operations.

City of Charlotte Response

The City recognizes that the 700 MHz Public Safety broadband spectrum is allocated to mobile use in recognition of the need for discrete spectrum for mobile uses. Additionally, the City is also aware that operation of fixed services in this band is permitted only on an ancillary basis. The City intends to deploy CharMeck Connect to support Public Safety use in a mobile environment and intends to minimize any fixed-station use of these frequencies and such fixed devices will be permitted only on a secondary, non-interference basis to the primary mobile operations.

Performance

Requirements

Early-deployed systems must satisfy baseline operability requirements in order to successfully interoperate with other networks. For instance, high spectral efficiency and network performance will enable the delivery of broadband services, including access to the common set of applications required in the *700 MHz Waiver Order*, to the largest possible number of users given the available spectrum resources. ERIC requires Petitioners' systems to meet baseline performance requirements, namely that they provide outdoor coverage at minimum data rates of 256 Kbps uplink (UL) and 768 Kbps downlink (DL), for all types of devices, for a user at the cell edge. Petitioners' systems should provide the minimum data rates, based on a sector loading of seventy percent, throughout the entire network. Each Petitioner should be required to certify its compliance with these requirements in the quarterly report that follows its date of service availability. This certification must be based on a representation of the actual "as-built" network and accompanied by UL and DL data rate plots that map specific performance levels, to include 256 Kbps UL and 768 Kbps DL.

City of Charlotte Response

The CharMeck Connect 700 MHz Public Safety Wireless Broadband Network is designed to provide outstanding performance and coverage to Public Safety users throughout the City of Charlotte and Mecklenburg County. A total of 39 eNodeB transmit/receive sites will be deployed throughout the County to provide the desired level of coverage. The system is designed to deliver 3 Mbps and 6 Mbps aggregate sector throughput for uplink and downlink connections respectively. These values are equivalent to the expected bandwidth, or capacity, available to all users within a single sector using the current 10 MHz spectrum allocation.

Three levels of coverage are planned for CharMeck Connect in order to meet the operational requirements of the City/County and other Public Safety users.

1. "**Mobile Coverage**" to a vehicle-mounted modem will be provided throughout Mecklenburg County with minimum throughput of 256 Kbps UL and 768 Kbps DL for a single user at the cell edge at vehicular speeds of 80 miles per hour.
2. "**Urban Portable Coverage**" using a portable device or USB dongle within a light to medium building will be provided over a defined geographic area of the City of Charlotte, with minimum throughputs of 256 Kbps uplink and 768 Kbps downlink for a single user at the cell edge at walking speeds.
3. "**Dense Urban Portable Coverage**" using a portable device or USB dongle within a dense building will be provided over a defined geographic area within downtown Charlotte, with minimum throughputs of 256 Kbps uplink and 768 Kbps downlink for a single user at the cell edge at walking speeds.

Each of the three levels of coverage will be provided assuming a sector loading of 70% and a confidence reliability of 95%. Per ERIC's recommendations on resources loading, in particular the 70% loading criteria, 70% load is reflected in both uplink and downlink designs as follows:

- In the uplink interference from outer cells, or so-called Interference-over-Thermal, will translate into a ~5dB noise floor rise. Such interference would be caused by identical physical resource blocks being used in adjacent cells In the downlink it translates into

70% of resources blocks being used in adjacent cells

Coverage maps were obtained through the use of a radio planning tool, which includes terrain and clutter data information and is typically used by commercial service providers. The system budget parameters and sites locations are used as input drivers to the tool with propagation modeling achieved through drive testing in regions with similar characteristics. Post-contract award field engineers will attempt to meet and perfect the preliminary design based on real field conditions before the initiation of coverage testing procedures.

Coverage plots depicting the predicted coverage for each of the three areas described above are provided in Appendix A

The City has established an extensive coverage verification test procedure that will record and verify coverage performance in-street and in specific facilities, using a grid testing approach consistent with industry standards. The City will share with the FCC the test results from each of the three areas as they are recorded and verified.

Coverage

Requirements

As an important step in promoting the Commission's long-standing goal of widespread coverage for public safety broadband networks, the Commission requires Petitioners to provide a plan for achieving significant population coverage within their jurisdictions within ten years of their date of service availability.

City of Charlotte Response

The City's plan for CharMeck Connect is to provide substantial coverage (greater than 97%) of the population of Mecklenburg County following completion of Phase 2 of the implementation, which is scheduled for July 2013. Additionally, the network will be expanded beyond this initial deployment to surrounding municipalities and counties using a common and cost-effective network backbone and core.

Coverage Reliability

Requirements

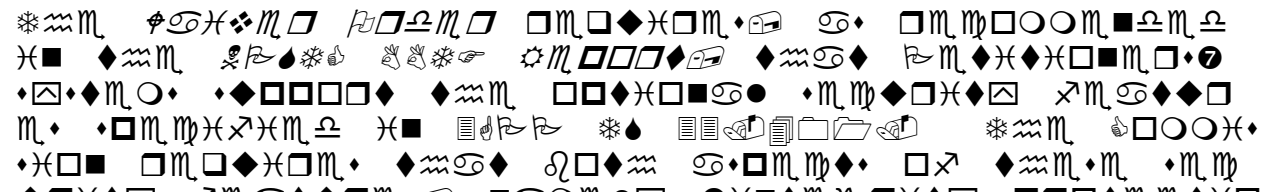
Network availability is a critical factor in ensuring that early-deployed networks are both operable and interoperable during emergency situations. ERIC therefore recommends that the Commission require Petitioners' systems provide a probability of coverage of 95 percent for all services and applications throughout the network. ERIC notes that this requirement finds support in several of Petitioners' interoperability showings, and it is a standard commonly used today by the Land Mobile Radio and Cellular industries.

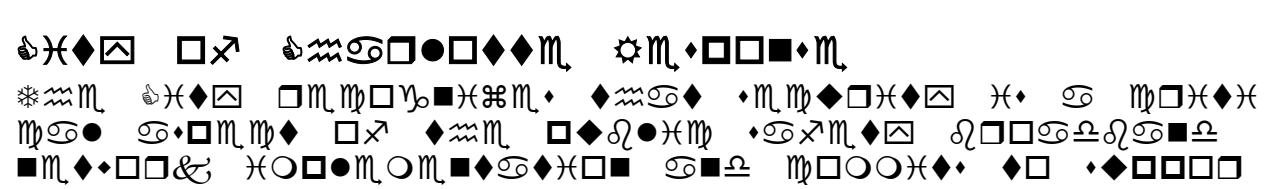
City of Charlotte Response

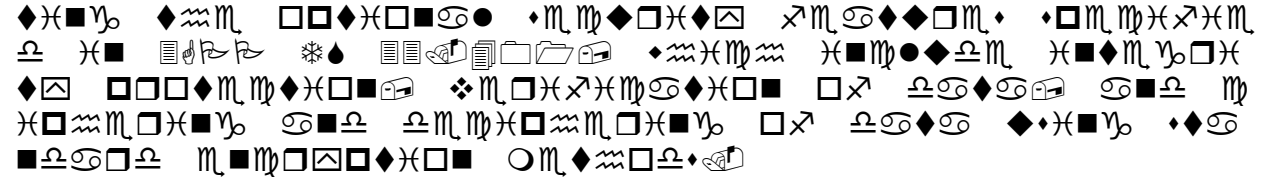
The CharMeck Connect 700 MHz Public Safety Wireless Broadband Network has been designed for the coverage requirements stated above with confidence reliability of 95%, as is commonly done for the design of Public Safety mission critical systems. Per ERIC's recommendations the system link budget accounted for a 95% area coverage reliability corresponding to some amount of shadowing margin and handoff margin. No additional fade margin, beyond consideration for portability, indoor service or external (intra-system) LTE interference, was considered.

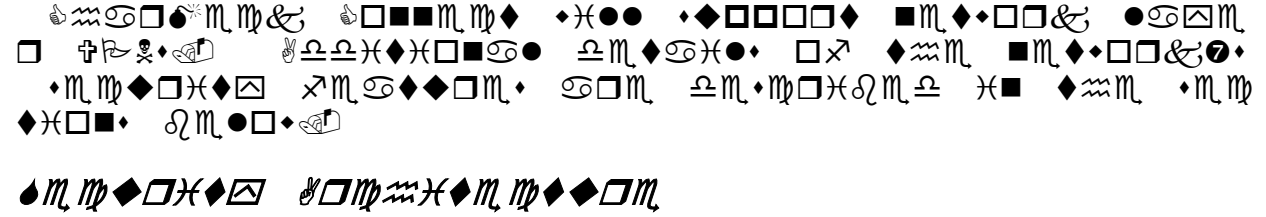
Security and Encryption

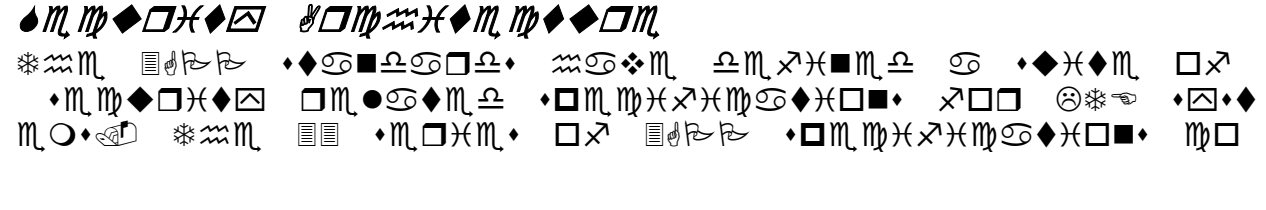
&$(&#%*&&)&*)*

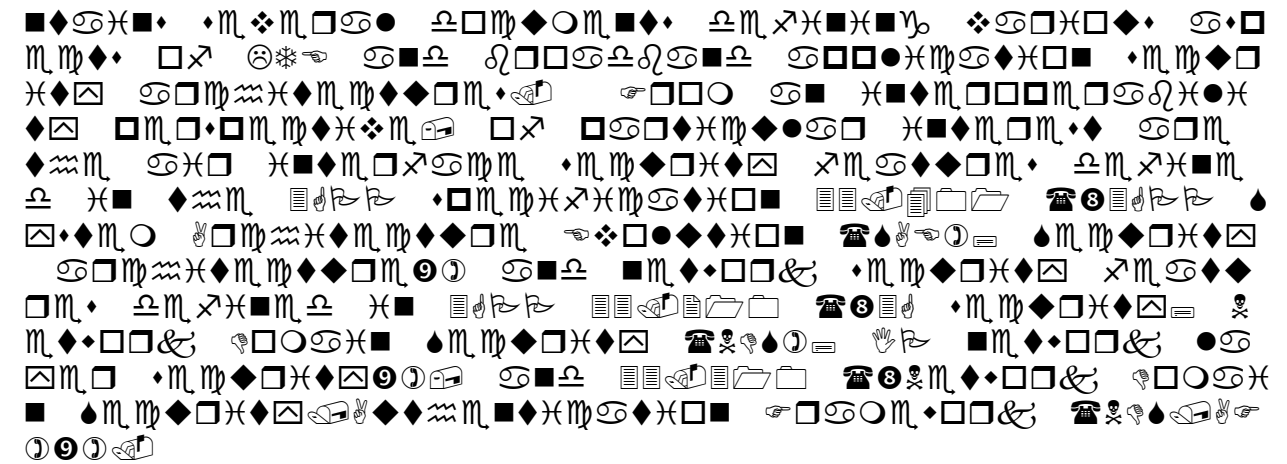


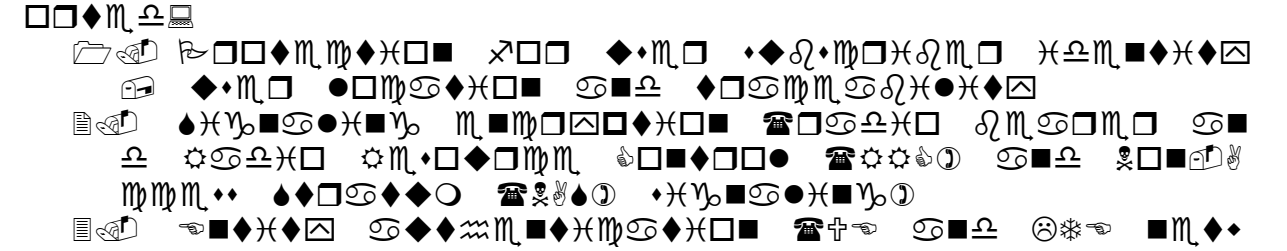


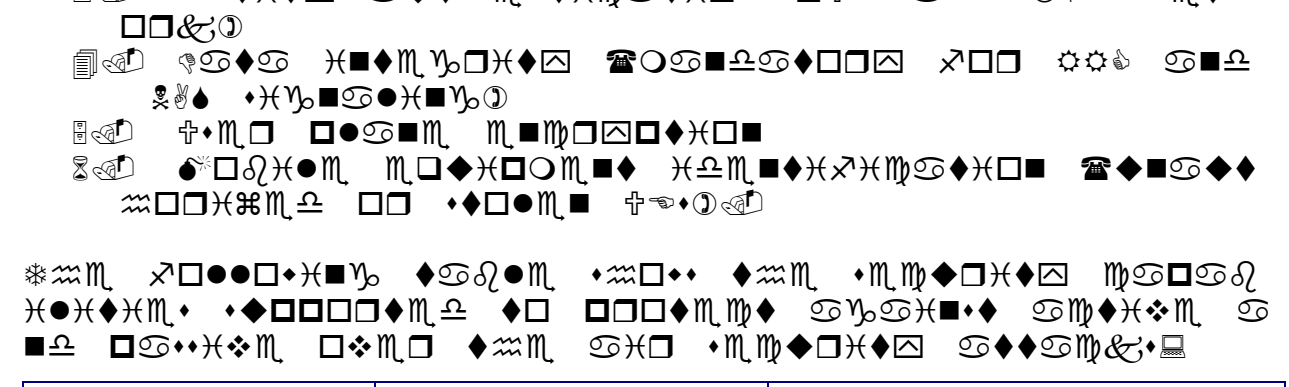


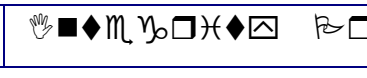
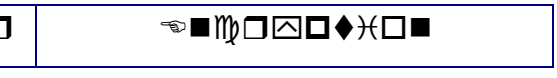










Interference Mitigation

Requirements

In addition to the coordination requirements set forth in the 700 MHz Waiver Order, The Commission requires Petitioners to employ interference mitigation techniques that will avoid signal/spectral efficiency degradation within a region and between overlapping or adjacent regions. Specifically, the Commission requires each Petitioner to implement the static Inter-Cell Interference Coordination (ICIC) feature among its eNodeBs by its date of service availability to ensure that its network operates without interference.

City of Charlotte Response

CharMeck Connect has been designed in accordance with FCC rules and 3GPP specifications and engineered so not to interfere with existing authorized systems. Static ICIC implies restrictions over a specific set of radio resources in order to minimize interference at the edge of a cell. This works well for traffic channels, but may create problems when used with control channels. In the case of the downlink control channel, the main Physical Downlink Control Channel (PDCCH) occupies the whole band, whereas, over the uplink, the Physical Uplink Control Channel (PUCCH) signals are at the edge of the band, except in the case of the Over-Provisioned PUCCH scheme. Therefore, the City of Charlotte and Alcatel-Lucent do not recommend utilizing the pre-provisioned static ICIC mechanism for public safety deployments due to the dynamic nature of incidents whereby traffic loads can shift from one cell to another simply because of the nature of these incidents. The City believes that Frequency Selective Scheduling (FSS) is better suited for this dynamic environment for both intra and inter-jurisdictional interference mitigation. With this technique, adjacent neighbor cells are treated in the same fashion as adjacent intra-jurisdictional cells. Followin

[illegible]

Out of Band Emissions

Requirements

The FCC requires that, for operations in the 763-768 MHz band and the 793-798 MHz band, the power of any emission outside the lessee's frequency band(s) of operation shall be attenuated below the transmitter power (P) within the licensed band(s) of operation, measured in watts, in accordance with the following:

- On any frequency outside the 763-768 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) dB;
- On any frequency outside the 793-798 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) dB

City of Charlotte Response

CharMeck Connect will utilize LTE radio nodes from Alcatel-Lucent which comply with out-of-band emissions limits per Part 27 and Part 90, and as specified in the Waiver Order, 3rd Report &Order and 4th FNPRM released in 01/26/2011. In particular, the radio equipment was granted authorization on 10/21/2011 under FCC id AS5BBTRX-04. The equipment was shown to meet and exceed the OOBE requirement when transmitting in the D-block, the PSBB block or the combined D+PSBB block.

CONCLUSION

The City of Charlotte asserts that its CharMeck Connect 700 MHz Public Safety Wireless Broadband Network is designed and is being implemented to meet or exceed the interoperability and other requirements of applicable FCC Orders. The table below summarizes compliance to the specific requirements. CharMeck Connect will support Sub-Network Mobility as of its Service Availability date on June 30, 2012. The City of Charlotte plans to amend this InterOperability Showing (IOS) approximately mid-February 2012 to reflect evolving information from activities of the PSST-OAC as well as other interworking and collaboration efforts. Given the above, the City believes it has made sufficient progress in its deployment and conformance to FCC requirements such that the renewal of its 700 MHz waiver later this year is easily justified. The City of Charlotte and its vendor Alcatel-Lucent have developed flexible designs to accommodate the IIG guidelines and other developing aspects. The updated timeline in Appendix C should be kept in consideration by the Commission in order for Charlotte to meet it's Service Availability date.

COMPLIANCE SUMMARY (Augmented per DA 12-25)

	Requirement		Comment
1	Public Safety Sub-Network Mobility (Technical 'roaming' for home routed and local breakout; 'intra-system' roaming)	C	
2	Commercial Roaming (Not required at Service Availability Date)	P	Target mid-2013
3	Support interfaces necessary to ensure the interoperability of equipment and devices manufactured by different vendors	C	
4	IPv4 on Service Availability; IPv6 later	C	Applicable IPv6 support at SA
5	System Identifiers (PLMN & other IDs & numbering schema)	C	
6	LTE Release 8 and higher of 3GPP standards	C	Release 9 implementation
7	PCS.TCRB + PSCR Conformance Testing	C	FCC activity awaited
8	InterOperability Testing (IOT – systems interfaces)	C	
9	Operation of Fixed Stations	C	
10	ERIC Baseline Performance Requirements	C	Meet requirements at SA Date
11	Plan for achieving significant population coverage	C	Substantial coverage (>97%)
12	System coverage reliability > 95 percent	C	
13	Support key security features in 3GPP TS 33.401	C	
14	Employ interference mitigation techniques	C	
15	Out Of Band Emissions compliance	C	
16	Implement ATIS-IOC Common PLMN ID	C	
17	IMSI and other Numbering Scheme Implemented	C	
18	Implement Common Clearinghouse (**Commercial Carrier Network Roaming**; not required at Service Availability Date)	P	Target mid-2013

C = City of Charlotte does comply with requirement at Service Availability Date

P = City of Charlotte will comply with requirement during in Phase 2 of project

APPENDIX A: COVERAGE MAPS

The predicted maps illustrated herein describe the projected coverage under current design assumptions. While not explicit, the impact of building obstructions and the like is accounted for by the clutter data hence the mapping onto different morphology classes (e.g. dense-urban, urban, suburban, rural).

APPENDIX B: DEFINITIONS / EVOLUTION OF TERMINOLOGY

Please refer also to page 14. The Public Safety Spectrum Trust Operating Advisory Committee LTE Infrastructure Internetworking Group (IIG) has evolved the public safety LTE terminology currently in use as referenced originally in the Federal Communications Commission Report & Orders (R&O's). As a result of architectural and other discussions related to implementing interworking as required by FCC R&Os and NPRMs, the LTE IIG has found it necessary to evolve and refine the original definitions. The following are the most salient refinements of the terminology. Some, but not all of the material within this InterOperability Showing (IOS) has been adapted to include the refinements in terminology.

- Public Safety Broadband Network – The entire Public Safety LTE Network with a Common PLMN-ID which is comprised of many small sub-networks.
- Public Safety Sub-Network - A subset of the Public Safety Broadband Network defined by an IMSI/MSIN range within the Common (single) PLMN-ID. A sub-network provides an HSS for its particular IMSI Range within the Common PLMN ID. Each Sub-network has an HSS. The National Network is subdivided into Sub-Networks based on IMSI ranges within that Common (single) PLMN-ID. By definition, each Sub-Network is operated by a different Public Safety agency or agencies. DIAMETER protocols and routing (DRA) ensure that MME's know the appropriate HSS to work with.
- Public Safety Sub-Network Mobility – Movement of a user between sub-networks. Service availability across sub-networks is provided by IMSI-range and APN node-selection functionality. This is mobility within the same Common PLMN ID. This is also known as Intra-System Roaming.
- Home PGW Access (HPA) - Accessing Home APNs from visited sub-network. As opposed to Home Routed Traffic when Roaming to/from carrier networks with a different PLMN ID.
- Local PGW Access (LPA) - Accessing common APNs via local PGWs in a visited sub-network. Common APNs need to be implemented in each sub-network. As opposed to Local Breakout (LBO) Traffic when Roaming to/from carrier networks with a different PLMN ID.
- Roaming – Movement of a user between the systems of different PLMN IDs. This typically would be Inter-System Roaming with commercial carriers. There is no handover across PLMN ID boundaries in a roaming scenario.
- Handover – Movement of a user between LTE Cells or Radio Access Technologies. However, Radio Access Technology (RAT) Handover is not likely to apply in PS LTE scenarios.

APPENDIX C: HIGH LEVEL PROGRAM DATES

FCC REQUIREMENTS BY PHASE [Refer to Compliance Summary in CONCLUSION]

FCC Requirement or Related Action	Phase
All except Commercial Roaming & Clearinghouse Implementation	Phase 1
Commercial Roaming & Clearinghouse Implementation	Phase 2 (Approx 2Q2013)
Numbering Administrator Implemented (Target)	Phase 1 March 2012
IPX Identified & Contracted (Target Date)	Phase 1 April 2012
Commercial Clearinghouse Identified (Target)	Phase 2 3Q12

CITY OF CHARLOTTE TIMELINE

Milestone	Completion Date
Devices RFQ Released	**COMPLETED**
Devices Vendor(s) Selected	**COMPLETED**
Interoperability Testing (Device) START	**COMPLETED**
RF & Microwave Designs Complete	**COMPLETED**
Common PLMN ID Committed	**02/24/12**
Phase 1: Site Development (DNC 7 sites)	03/05/12
IMSI Ranges Allocated to City of Charlotte	**03/15/12**
LTE RF Design & Preliminary Activities	03/15/12
Interoperability Testing Devices Complete	03/30/12
FCC authorization for PLMN ID & numbering	**03/30/12**
Core & Network Management Installation	04/25/12
Phase 1 Cell Site Install (DNC 7 sites)	05/09/12
Phase 2: Site Development (32 sites)	05/21/12
Data Core/Network Mgmt Integration	05/23/12
Phase 1: eNodeB Integration	05/23/12
Phase 1: RF Coverage Verification	06/12/12
Phase 1: Perform System Testing	06/27/12
Phase 1: Customer Acceptance	06/28/12
Phase 1: Go-Live (DNC) **SERVICE AVAILABILITY DATE**	**06/30/12**
Phase 2 Cell Site Install (32sites)	01/04/13
Phase 2: eNodeB Integration	02/15/13
Phase 2: RF Coverage Verification	04/01/13
Phase 2: Perform System Testing	05/15/13
Phase 2: 60 Day Burn In	07/18/13
Phase 2: Customer Acceptance	07/25/13

APPENDIX D: RESPONSE REGARDING ORDER DA 12-25

On January 9th, 2012, subsequent to City of Charlotte's January 5th filing, the Commission's Public Safety and Homeland Security Bureau, acting in consultation with its Emergency Response Interoperability Center (ERIC), adopted Order DA 12-25 which provides further guidance to 700 MHz public safety broadband waiver recipients (including City of Charlotte) on their implementation of a public land mobile network identifier (PLMN ID) and related network identification numbering scheme to support the interoperability of the network deployments.

The main body of this InterOperability Showing has been rewritten to reflect the new information. This Appendix D documents the incremental information of City of Charlotte's response & intentions relative to this Order.

. Charlotte will follow the Commission's direction to implement the Common PLMN ID and to follow the PSCR guidance as modified by the PSST-OAC Numeric Identifierg working group. City will work with the other early system implementers to identify a numbering administrator and complete the numbering scheme. Charlotte will identify a clearing house; however inter-system roaming itself is not Phase 1 scope.

SPECIFIC IMPLEMENTATION ASPECTS

- The City of Charlotte will implement, prior to its date of service availability on 6/30/12 a common PLMN ID that the ATIS IMSI Oversight Council (ATIS IOC) designates for the 700 MHz public safety broadband network.
- The implementation of a Common PLMN ID was assumed previously. Substantial high-level and low-level design work has been completed based upon this requirement. Charlotte's commitment to the Common PLMN ID is thus demonstrated.
- City of Charlotte has been and is currently a participant in the PSST-OAC Numeric Identifier working group for the implementation of the numbering schema. Charlotte, with this working group and with other Waiver Recipients, will collectively implement the schema for the assignment of IMSIs and other identification numbers necessary to support all of the Waiver Recipients' operations of LTE broadband deployments on an interoperable basis. Charlotte's commitment to a common numbering schema is therefore indicated.
- The City of Charlotte is a leading participant in the LTE IIG. The LTE Infrastructure Internetworking Group (IIG) is a team of industry consultants, LTE infrastructure providers and network operators selected by the PSST-OAC to develop recommendations on guidelines for internetworking and a plan by which the PSST-OAC jurisdictions can establish internetworking. City of Charlotte plans to adhere to these recommendations. Charlotte's commitment to broad support of all of the Waiver Recipients' operations of LTE broadband deployments on an interoperable basis is therefore indicated.
- Commercial Roaming (equivalent to Public Safety Inter-System Roaming) does not currently exist. This IIG workscope is currently scheduled beyond February 2012.
- City of Charlotte is currently working with PSST-OAC and the Waiver Recipientss to identify and retain a competent numbering administrator. The City of Charlotte had previously, in December 2011 and in conjunction with the PSST-OAC IIG, initiated a Request For Information (RFI) regarding IPX Interworking and Network Services. An

RFI objective is to arrange for a common competent clearinghouse to support commercial roaming by all of the Petitioners. As stated in this Interoperability Showing, inter-system commercial roaming has been anticipated and substantial high-level and low-level design work has been completed based upon these requirements. City of Charlotte's commitment to a common clearinghouse is thus demonstrated. Support for such will be in Phase 2.

- City of Charlotte may initially direct connect (S6a & S5 interfaces) to the Harris County, Texas systems while awaiting IPX services providers to be contracted.